

**PEMBUATAN APLIKASI WEB VULNERABILITY SCANNER  
TERHADAP KELEMAHAN XSS (Cross Site Scripting)  
MENGUNAKAN JAVA.**

**TUGAS AKHIR**



**Oleh :**

**M. TRI JOKO**  
**0534010093**

**JURUSAN TEKNIK INFORMATIKA  
FAKULTAS TEKNOLOGI INDUSTRI  
UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN”  
JAWA TIMUR  
2010**

**PEMBUATAN APLIKASI WEB VULNERABILITY SCANNER  
TERHADAP KELEMAHAN XSS (Cross Site Scripting)  
MENGUNAKAN JAVA.**

**TUGAS AKHIR**

**Diajukan Untuk Memenuhi Sebagian Persyaratan  
Dalam Memperoleh Gelar Sarjana Komputer  
Jurusan Teknik Informatika**



**Oleh :**

**M. TRI JOKO  
0534010093**

**JURUSAN TEKNIK INFORMATIKA  
FAKULTAS TEKNOLOGI INDUSTRI  
UNIVERSITAS PEMBANGUNAN NASIONAL “VETERAN”  
JAWA TIMUR  
2010**

## KATA PENGANTAR

Alhamdulillah, dengan mengucapkan puji dan syukur kehadiran Allah SWT atas rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan tugas akhir ini dengan judul “PEMBUATAN APLIKASI WEB VULNERABILITY SCANNER TERHADAP KELEMAHAN XSS (Cross Site Scripting) MENGGUNAKAN JAVA “yang merupakan persyaratan dalam memperoleh gelar Sarjana Komputer di Universitas Pembangunan Nasional “VETERAN” Jatim.

Penulis mengucapkan terima kasih yang sebesar-besarnya kepada pihak-pihak yang telah membantu baik materiil maupun dorongan spirituil untuk menyelesaikan penulisan kerja praktek ini, terutama kepada:

1. Orang Tua dan keluarga tercinta serta sayangku nenni sutomo atas motivasi dan doanya sehingga semua yang dikerjakan dapat berjalan lancar.
2. Bapak Prof. Dr. Ir. Teguh Soedarto, MP, selaku Rektor UPN “Veteran” Jatim.
3. Bapak Ir. Bambang Wahyudi, MS, selaku DEKAN FTI UPN “VETERAN” Jatim.
4. Bapak Nur Cahyo Wibowo, S.Kom, M.Kom selaku Kepala Jur. Sistem Informasi, FTI UPN “VETERAN” Jatim.
5. Bapak Basuki Rachmat, S.Si, MT, selaku Kepala Jurusan Teknik Informatika sekaligus Tim Penguji Tugas Akhir Penulis.
6. Bapak Achmad Junaidi, S.Kom, selaku Dosen Pembimbing yang telah meluangkan waktu untuk memberikan bimbingan selama proses pelaksanaan Tugas Akhir penulis.

7. Bapak Chrystia Aji P, S.Kom, selaku Dosen Pembimbing yang telah meluangkan waktu untuk memberikan bimbingan selama proses pelaksanaan Tugas Akhir penulis.
8. *Special to*: Arbi Septiawan (pakde) dan my laptop yang selalu setia menemani untuk mengerjakan ini semua..
9. Dosen-dosen Teknik Informatika dan Sistem Informasi, *staff* dan segenap civitas akademika UPN “VETERAN” Jatim.
10. *My best Friends*: Diah, Indri, Rina, Ve, Amey, MIO *Gangster* (Bang Budi abangku tercinta, Broden, Jo2, Faisal, Ringgo, Mr. Craps, Pak Cahyo, Max, and buat semuanya teman-teman UPN ).
11. MITRA IT (BGJUNCTION L2-B23), Pak Wahyudi makasih untuk tempatnya, Frangky, Ito yang slalu setia menemani, semua *crew* Yogyafree.net.
12. Teman-teman Perum Marinir Gunung Sari makasih untuk *suport* dan doanya dan Mas Mukhson makasih slalu kasih info.
13. Tidak lupa penulis ucapkan terima kasih kepada teman-teman yang tidak dapat disebutkan satu persatu atas segala bantuannya dalam menyelesaikan Tugas Akhir ini.

Penulis menyadari sepenuhnya masih banyak terdapat kekurangan dalam penulisan Tugas Akhir ini. Oleh sebab itu kritik serta saran yang membangun dari pembaca sangat membantu guna perbaikan dan pengembangan di masa yang akan datang.

Akhirnya dengan ridho Allah penulis berharap semoga Tugas Akhir ini dapat memberikan manfaat bagi pembaca sekalian terutama mahasiswa di bidang komputer.

Surabaya, 10 Agustus 2010

Penulis

## DAFTAR ISI

	Halaman
HALAMAN JUDUL	
LEMBAR PENGESAHAN	
LEMBAR PENGESAHAN DAN PERSETUJUAN	
KETERANGAN REVISI	
MOTTO	
ABSTRAKSI	
KATA PENGANTAR .....	ix
DAFTAR ISI .....	xiii
DAFTAR TABEL .....	xv
DAFTAR GAMBAR .....	xvi
BAB I PENDAHULUAN .....	1
1.1 Latar Belakang Masalah .....	1
1.2 Perumusan Masalah .....	3
1.3 Batasan Masalah .....	4
1.4 Tujuan .....	4
1.5 Manfaat Sistem Bagi Pengguna .....	4
1.6 Metodologi .....	5
1.7 Sistematika Penulisan .....	6
BAB II LANDASAN TEORI .....	8
2.1 Web .....	8
2.2 XSS (Cross Site Scripting) .....	12
2.2.1 Cara Kerja Cross Site Scripting .....	12

2.2.2 Web Site Dengan Cross Site Scripting .....	14
2.2.3 Informasi Yang Diterbitkan Penyedia Layanan .....	18
2.2.4 Link Dalam Cross Site Scripting .....	19
2.2.5 Pencurian Data .....	20
2.2.6 Apa Yang Cross Site Scripting Dapat Lakukan .....	21
2.3 Java .....	23
2.4 PHP.....	29
2.5 MY SQL .....	34
2.6 HTML (Hyper Text Markup Language) .....	36
2.6.1 Struktur HTML .....	37
2.7 Web Server .....	39
2.7.1 Cara Kerja Web Server .....	40
<b>BAB III PERANCANGAN .....</b>	<b>42</b>
3.1 Desain Sistem .....	42
3.2 Perancangan Sistem .....	43
3.3 Perancangan Data Input.. .....	44
3.4 Perancangan Proses .....	45
3.4.1 Proses Scanning .....	45
3.5 Perancangan Antar Muka .....	49
3.5.1 Blok Arsitektur Sistem WVS Online .....	49
3.5.2 Blok Arsitektur sistem WVS berbasis Offline .....	50
<b>BAB IV IMPLEMENTASI .....</b>	<b>52</b>
4.1 Implementasi Sistem .....	52

BAB V PENGUJIAN DAN ANALISA .....	57
5.1 Lingkungan Pengujian .....	57
5.2 Uji Coba .....	57
5.2.1 Aplikasi Web Vulnerability Scanner .....	57
5.2.2 Proses Scanning Secara Online .....	59
5.2.3 Proses Scanning Secara Offline .....	78
5.3 ANALISA .....	81
5.3.1 Analisa Scan XSS .....	81
BAB VI PENUTUP.....	84
6.1 Kesimpulan.....	84
6.2 Saran.....	84



## DAFTAR TABEL

	Halaman
Tabel 2.1 Perbandingan Antara Static Dengan Dynamic Web Page...	9
Tabel 2.2 HTML Escape Encoding.....	15
Tabel 2.3 Tipe Data Dalam My SQL.. .....	30

## DAFTAR GAMBAR

	Halaman
Gambar 1.1 Data Statistik Serangan Terhadap Aplikasi Web .....	2
Gambar 2.1 Alur Data Tipikal Untuk Halaman Web Yang Statis.....	8
Gambar 2.2 Contoh Alur Data Pada Halaman Web Yang Dinamis.....	10
Gambar 2.3 Contoh Kasus Cross Site Scripting.....	12
Gambar 2.4 Contoh Kasus Cross Site Scripting .....	14
Gambar 2.5 Contoh Kasus Cross Site Scripting .....	14
Gambar 2.6 Contoh Kasus Cross Site Scripting .....	18
Gambar 2.7 Contoh Kasus Cross Site Scripting .....	19
Gambar 2.8 Cara Kerja Web Server .....	33
Gambar 3.1 Perancangan Sistem Secara Global .....	36
Gambar 3.2 Diagram Alur Scan XSS .....	38
Gambar 3.3 Proses Injeksi XSS Tidak Valid .....	40
Gambar 3.4 Proses Injeksi XSS Valid .....	41
Gambar 3.5 Blok Arsitektur Sistem WVS berbasis online .....	42
Gambar 3.6 Blok Arsitektur Sistem WVS berbasis offline .....	43
Gambar 4.1 Tampilan Menu Utama .....	44
Gambar 4.2 Halaman WVS Scan XSS .....	45
Gambar 4.3 Potongan Script Scan XSS .....	45
Gambar 4.4 Tampilan Laporan Scan XSS .....	46

Gambar 4.5	Laporan Scanning Terakhir .....	46
Gambar 4.6	Potongan script laporan scanning terakhir .....	47
Gambar 4.7	Fitur Help .....	48
Gambar 5.1	Form Halaman Utama .....	50
Gambar 5.2	Tampilan Awal Website Target .....	51
Gambar 5.3	Form Scanning XSS .....	52
Gambar 5.4	Proses Scan XSS Telah Selesai .....	53
Gambar 5.5	Laporan Scan XSS .....	53
Gambar 5.6	Tampilan Awal Website Yang Sudah Terinjeksi XSS .....	54
Gambar 5.7	Tampilan Awal Website Target .....	55
Gambar 5.8	Form Scanning XSS .....	55
Gambar 5.9	Proses Scan XSS Telah Selesai .....	56
Gambar 5.10	Laporan Scan XSS .....	57
Gambar 5.11	Tampilan Awal Website Yang Sudah Terinjeksi XSS` .....	57
Gambar 5.12	Tampilan Awal Website Target .....	58
Gambar 5.13	Form Scanning XSS .....	59
Gambar 5.14	<i>Proses Scan XSS telah selesai</i> .....	60
Gambar 5.15	Laporan Scan XSS .....	60
Gambar 5.16	Tampilan Awal Website Yang Sudah Terinjeksi XSS` .....	61
Gambar 5.17	Tampilan Awal Website Target .....	62
Gambar 5.18	Form Scanning XSS .....	63
Gambar 5.19	<i>Proses Scan XSS telah selesai</i> .....	63
Gambar 5.20	Laporan Scan XSS .....	64

Gambar 5.21	Tampilan Awal Website Yang Sudah Terinjeksi XSS` .....	64
Gambar 5.22	Tampilan Awal Website Target .....	65
Gambar 5.23	Form Scanning XSS .....	66
Gambar 5.24	<i>Proses Scan XSS telah selesai</i> .....	67
Gambar 5.25	Laporan Scan XSS .....	67
Gambar 5.26	Tampilan Awal Website Yang Sudah Terinjeksi XSS` .....	68
Gambar 5.27	Tampilan Website Tiruan .....	69
Gambar 5.28	Tampilan Awal Website Target .....	70
Gambar 5.29	Form Scanning XSS .....	71
Gambar 5.30	<i>Proses Scan XSS telah selesai</i> .....	72
Gambar 5.31	Laporan Scan XSS .....	72
Gambar 5.32	Tampilan Awal Website Yang Sudah Terinjeksi XSS` .....	73
Gambar 5.33	Halaman URL yang telah di injeksi .....	75

## **ABSTRAKSI**

*Hingga saat ini tindakan penyerangan pada suatu web semakin tinggi. Sering terlihat di media cetak, dan media elektronik begitu banyak berita yang memuat aksi-aksi penyerangan terhadap suatu situs web. Salah satu contoh faktor timbulnya tindakan hacking adalah kesalahan dalam scripting pembuatan web adalah hal terbanyak yang dimanfaatkan oleh para attacker, sehingga rata-rata web yang berhasil diserang melalui lubang ini. Kelemahan-kelemahan scripting yang ditemukan pada proses vulnerabilities scanning misalnya, XSS.*

*Untuk mencegah tindakan tersebut dapat menggunakan jasa perusahaan audit keamanan web. Dan tentunya akan menghabiskan banyak biaya, untuk menghindari hal tersebut, dalam proyek akhir ini akan dibangun aplikasi web vulnerability scanner yang berfungsi untuk mendeteksi suatu kelemahan web terhadap kelemahan XSS.*

*Maka dengan menggunakan aplikasi web vulnerability scanner dapat dideteksi suatu kelemahan web terhadap kelemahan XSS dengan lebih dini sehingga dapat dicegah. Untuk kedepannya aplikasi web vulnerability scanner dapat digabungkan dengan browser.*

**Kata kunci** : XSS ,Web Vulnerability Scanner Java.

# BAB I

## PENDAHULUAN

### 1.1 LATAR BELAKANG

Perkembangan dalam dunia maya terjadi sangat pesat. Teknologi baru dirancang dan diimplementasikan untuk memenuhi kebutuhan pengguna yang semakin beragam. Teknologi halaman *web* termasuk didalamnya. Teknologi yang ada kini telah ber-revolusi menuju ke tingkatan yang berbeda. Halaman *web* kini tidak lagi statis namun juga dinamis. Kini halaman *web* yang dinamis merupakan pemandangan yang biasa kita lihat ketika melakukan *surfing* menggunakan *internet*.

Halaman *web* yang dinamis merupakan teknologi yang memberi perubahan penyediaan informasi, layanan, dan tampilan secara signifikan. Halaman *web* yang dinamis memungkinkan interaksi yang lebih baik antara penyedia layanan dengan penggunanya. Dengan menggunakan teknologi ini, halaman *web* akan terlihat lebih manusiawi. Penyedia layanan dapat menambahkan content-content yang sebelumnya masih merupakan impian belaka.

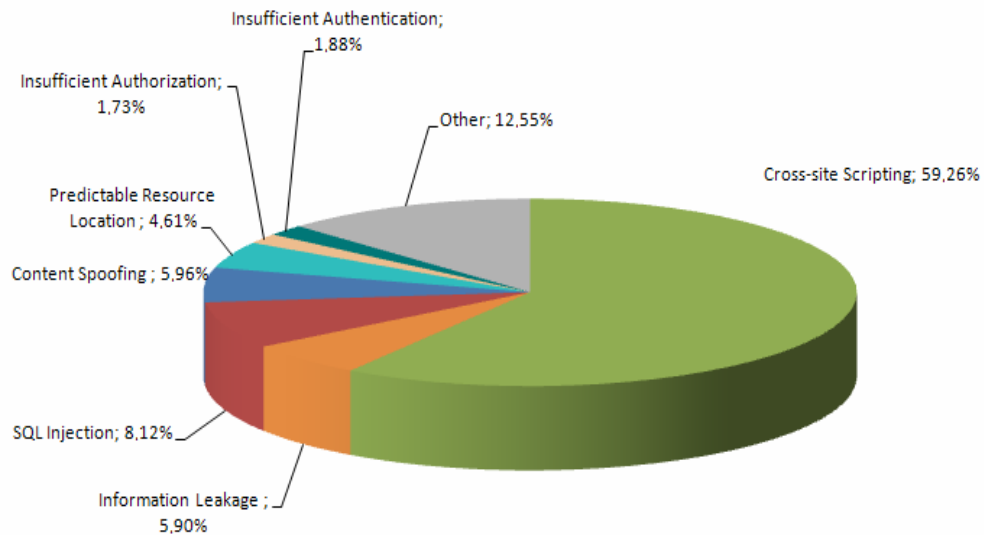
Dalam *system security computer*, istilah *Vulnerability* merupakan suatu kelemahan yang memungkinkan seseorang untuk masuk dan mendapatkan hak akses ke dalam komputer yang dituju(target). Biasanya *vulnerability* adalah kelemahan yang dikarenakan kesalahan setting ataupun ataupun ketidaktahuan administrator.(<http://ahmad-prayitno.com>)

Dan hingga saat ini angka kejahatan di dunia maya tetap tinggi dan terus meningkat. Sebuah penelitian yang dilakukan oleh *Corsaire* menunjukkan bahwa sekitar 25% aplikasi berbasis *web* memiliki celah yang membuatnya jadi rentan terhadap serangan yang dilakukan oleh para *cracker*. *Corsaire* mendasarkan hasil temuan ini pada penelitian selama enam tahun terakhir. (<http://berita.kapanlagi.com>)

Dalam menganalisa, *Corsaire* menggunakan sampel dari perusahaan-perusahaan besar di beberapa tempat termasuk *Inggris, Australia, Eropa, Asia* dan tentu saja Amerika Serikat. Hasil analisa menunjukkan bahwa meski ada usaha

untuk memperbaiki aplikasi berbasis *web* ini, namun setidaknya masih ada sekitar 25% yang memiliki resiko tinggi.

Berikut merupakan data dari <http://www.webappsec.org/projects/statistics> tentang statistic serangan terhadap Aplikasi Web:



**Gambar 1. 1** Data Statistik Serangan terhadap Aplikasi Web

Dari statistik diatas diketahui bahwa serangan XSS menempati urutan Pertama. Para *hacker* berkonsentrasi melakukan *eksploitasi* pada *web-web* di *internet*. *Web* yang tidak aman memberikan kemudahan akses kepada *hacker* untuk memanipulasi informasi dan melakukan aktivitas ilegal dengan menggunakan *situs* yang telah diserang. *Situs* yang menjadi korban dapat disalahgunakan untuk melakukan aktivitas kriminal. Misalnya saja melakukan *phishing*, pencurian informasi sensitif milik pengguna, memanen *email* pengguna untuk keperluan *spamming*, dll. Dalam kondisi ini, *Attacker* dapat membuat agar pemilik sah-nya yang bertanggung jawab atas tindak kejahatan tersebut

Dilatarbelakangi permasalahan di atas, dalam proyek akhir ini dibangun sebuah aplikasi yang berfungsi sebagai pendeteksi terhadap kelemahan XSS pada suatu aplikasi *web*, sehingga dengan bantuan aplikasi tersebut suatu aplikasi *web* dapat dideteksi lebih dini terhadap kelemahan XSS.

Selain itu, aplikasi ini juga memberikan info letak kelemahan suatu *web* terhadap serangan XSS. Dengan aplikasi ini, pengguna bisa mendeteksi apakah *web* memiliki kelemahan XSS atau tidak.

## 1.2 RUMUSAN MASALAH

Dari latar belakang masalah yang telah penulis paparkan, maka penulis mencoba untuk membangun aplikasi *Web Vulnerability Scanner*. Adapun beberapa rumusan permasalahan yang ada dalam membangun aplikasi *Web Vulnerability Scanner* ini yaitu :

- a) Bagaimana membangun ***Web Vulnerability Scanner*** berdasarkan data masukan dari pengguna berupa *URL* untuk *Web Vulnerability Scanner* berbasis *Online*.
- b) Bagaimana membangun ***Web Vulnerability Scanner*** berbasis *Offline* dengan ketentuan *file web* sudah harus tersimpan di *htdocs Xampp*.
- c) Bagaimana **Mengolah informasi dan menampilkan hasil scan** yang dibutuhkan oleh pengguna.

## 1.3 BATASAN MASALAH

Sedangkan batasan masalah pada proyek akhir ini, antara lain :

- a) Bahasa yang digunakan adalah *Java* dan *software developmentnya* adalah Netbeans
- b) Aplikasi *web* yang dapat di scan adalah aplikasi *web* yang dibangun dengan menggunakan bahasa pemrograman *PHP* dengan *MYSQL* sebagai *DBMS*.
- c) Kelemahan yang dibahas adalah XSS

## 1.4 TUJUAN

Tujuan proyek akhir ini adalah untuk membangun aplikasi *Web Vulnerability Scanner* Menggunakan *Java*. Adapun manfaat dengan dibangunnya aplikasi ini adalah untuk mendeteksi kelemahan *web* terhadap serangan XSS (*Cross Site Scripting*).

## 1.5 MANFAAT

Berdasarkan dari latar belakang diatas maka dapat dirumuskan masalah sebagai berikut :

- a. Membangun *web* secara *secure*.



Membuat *website* dengan tingkat keamanan yang tinggi sehingga tidak mudah untuk dirusak atau dimasuki oleh pihak – pihak tertentu.

b. Terhindar dari *defacer website*.

Adalah bebas dari para perusak tampilan pada *website* yang telah dibangun, bahkan menghapus seluruh data yang ada di dalam *database*.

c. Mendeteksi kelemahan *web* terhadap serangan XSS (*Cross Site Scripting*).

Yaitu mendeteksi salah satu jenis serangan *web* yang dilakukan dengan memanfaatkan kelemahan pada suatu aplikasi *web* sehingga memungkinkan aplikasi untuk menginjeksikan suatu tag *HTML* ataupun *Client Side Script* pada aplikasi *web* tersebut dikarenakan adanya variabel yang tidak disanitasi dengan baik.

## 1.6 METODOLOGI PENELITIAN

Dalam pengerjaan proyek akhir ini meliputi langkah-langkah sebagai berikut :

### 1. Studi Literatur

Pada tahap ini dilakukan studi literatur dari beberapa referensi baik itu dari buku atau internet.

### 2. Perancangan Sistem

Pada tahap ini dilakukan perancangan sistem yang akan dibangun, meliputi perancangan *database*, perancangan sistem dan pembuatan *user interface*.

### 3. Persiapan Data

Data-data penunjang yang didapatkan berupa suatu kesimpulan, fakta-fakta dan aturan yang mengatur proses pencarian data yang saling berhubungan satu sama lain disimpan ke dalam basis *data RMS (Record Management System)* sebagai media penyimpanan.

### 4. Pengujian dan Analisa

Pengujian dan analisa dimaksudkan untuk mengetahui sejauh mana sistem yang dibuat pada proyek akhir ini dapat berfungsi sesuai dengan proses sistem yang diharapkan.

### 5. Kesimpulan

Dibuat kesimpulan dari pengujian sistem proyek akhir dengan membandingkan apakah hasilnya seperti yang diharapkan pada tujuan proyek akhir sebelumnya.

## **6. Pembuatan Laporan**

Membuat dokumentasi dari semua tahapan proses diatas berupa laporan yang berisi tentang dasar teori, hasil proyek akhir dan hasil analisa.

### **1.7 SISTEMATIKA PENELITIAN**

Sistematika pembahasan yang akan diuraikan dalam buku laporan proyek akhir ini terbagi dalam beberapa bab yang akan dibahas sebagai berikut :

#### **BAB I PENDAHULUAN**

Bab ini berisi tentang pendahuluan yang terdiri dari latar belakang, perumusan masalah, batasan masalah, tujuan dan sasaran, metodologi, serta sistematika pembahasan dari Proyek Akhir ini.

#### **BAB II TEORI PENUNJANG**

Bab ini membahas mengenai teori-teori yang berkaitan dengan penyelesaian Proyek Akhir, yang didapatkan dari berbagai macam buku serta sumber-sumber terkait lainnya yang berhubungan dengan pembuatan Proyek Akhir ini.

#### **BAB III PERANCANGAN SISTEM**

Bab ini membahas mengenai perancangan sistem, meliputi perancangan hirarki, perancangan proses, dan perancangan *user interface*.

#### **BAB IV IMPLEMENTASI**

Bab ini membahas mengenai implementasi system

#### **BAB V UJI COBA DAN ANALISA**

Bab ini menyajikan dan menjelaskan seluruh hasil dan analisa dalam pembuatan Proyek Akhir ini dan bagaimana penyelesaian dari setiap permasalahan error yang terjadi pada sistem operasi Windows

## **BAB VI PENUTUP**

Bab ini berisi kesimpulan dari uji coba perangkat lunak, dan saran untuk pengembangan, perbaikan serta penyempurnaan terhadap aplikasi yang telah dibuat.